Office of the Secretary of Defense (OSD)
Office of Small Business Programs (OSBP)
15.3 Small Business Innovation Research (SBIR)
Proposal Submission Instructions

INTRODUCTION

The Army and Air Force are participating in the OSD SBIR Program on this solicitation. The Service laboratories act as OSD's agent in the management and execution of the contracts with small businesses.

Firms with strong research and development capabilities in science or engineering in any of the topic areas described in this section and with the ability to commercialize the results are encouraged to participate. Subject to availability of funds, the OSD SBIR Program will support high quality research and development proposals of innovative concepts to solve the listed defense-related scientific or engineering problems, especially those concepts that also have high potential for commercialization in the private sector. Objectives of the OSD SBIR Program include stimulating technological innovation, strengthening the role of small business in meeting DoD research and development needs, fostering and encouraging participation by minority and disadvantaged persons in technological innovation, and increasing the commercial application of DoD-supported research and development results. The guidelines presented in the solicitation incorporate and exploit the flexibility of the SBA Policy Directive to encourage proposals based on scientific and technical approaches most likely to yield results important to DoD and the private sector.

PROPOSAL SUBMISSION

In order to participate in the OSD SBIR Program, all potential proposers should register on the DoD SBIR/STTR Web site at https://sbir.defensebusiness.org/ as soon as possible. This site contains step-by-step instructions for the preparation and submission of the Proposal. It is required that all proposers submit their proposal electronically through the DoD SBIR/STTR Proposal Submission Web site at https://sbir.defensebusiness.org/. For general inquiries or problems with proposal electronic submission, contact the DoD SBIR Help Desk at 1-800-348-0787 (9:00 a.m. to 6:00 p.m. ET).

OSD WILL NOT accept any proposals that are not submitted through the on-line submission site. The submission site does not limit the overall file size for each electronic proposal; however, there is a 20-page limit for the Technical Volume. File uploads may take a great deal of time depending on your file size and your internet server connection speed. If you wish to upload a very large file, it is highly recommended that you submit your proposal prior to the deadline submittal date, as the last day is heavily trafficked. You are responsible for performing a virus check on each technical volume file to be uploaded electronically. The detection of a virus on any submission may be cause for the rejection of the proposal.

Proposals shall be submitted in response to a specific topic identified in the following topic description sections. The topics listed are the only topics for which proposals will be accepted.

In the OSD SBIR Program, Topic Authors are responsible for creating, submitting and revising topics for each solicitation. The Topic Author will be the primary point of contact and will have the following responsibilities:

- Selection of the Phase I proposals for contract award (in accordance with source selection procedures in the DoD solicitation,
- Managing the contract award,

- Notifying all of the small businesses who submitted of selection and non-selection in coordination with the contracting officer and the SBIR coordinator at the participating organization,
- Conducting debriefings as requested by those not selected (in coordination with the contracting officer and in accordance with the DoD solicitation) and,
- Annual reporting on contract execution.

During the Pre-release period, proposers have an opportunity to contact topic authors by telephone or e-mail to ask technical questions about specific solicitation topics, however, proposal evaluation is conducted only on the written proposal. Contact during the Pre-release period is considered informal, and will not be factored into the selection for award of contracts.

Following the pre-solicitation and in order to maintain source selection integrity, **no** direct contact between potential offerors and OSD SBIR/STTR technical personnel (including Topic Authors) is allowed during the Solicitation Period. However, offerors may submit written questions through the SBIR Interactive Topic Information System (SITIS), in which the questioner and respondent remain anonymous and all questions and answers are posted electronically for general viewing. Written questions to SITIS must be submitted at https://sbir.defensebusiness.org/sitis. Questions are limited to technical information related to improving the understanding of a particular topic's requirements; any other questions, such as those asking for advice or guidance on solution approach, will not receive a response. Questions received by the SITIS system are forwarded to the responsible Topic Author. SITIS opens simultaneously with the official opening of the solicitation and closes two weeks prior to the solicitation closing.

Key Dates

15.3 Solicitation Pre-Release	27 August 2015 – 27 September 2015
15.3 Solicitation Open & SITIS Opens	28 September 2015
15.3 SITIS Closes	14 October 2015
15.3 Solicitation Close	28 October 2015
15.3 Submission Deadline	28 January 2016 (by 6:00 am ET)
15.3 Award Goal	24 April 2016

PROPOSER ELIGIBILITY AND LIMITATIONS

Each proposer must qualify as a small business for research or research and development purposes and certify to this on the Cover Sheet of the proposal. In addition, a minimum of two-thirds of the research and/or analytical work in Phase I must be carried out by the proposing firm. For Phase II, a minimum of one-half (50%) of the research and/or analytical work must be performed by the proposing firm. The percentage of work is usually measured by both direct and indirect costs, although proposers planning to subcontract a significant fraction of their work should verify how it will be measured with their DoD contracting officer during contract negotiations. For both Phase I and II, the primary employment of the principal investigator must be with the small business firm at the time of the award and during the conduct of the proposed effort. Primary employment means that more than one-half of the principal investigator's time is spent with the small business. Primary employment with a small business concern precludes full-time employment at another organization. For both Phase I and Phase II, all research or research and development work must be performed by the small business concern and its subcontractors in the United States. Deviations from the requirements in this paragraph must be approved in writing by the contracting officer (during contract negotiations).

Joint ventures and limited partnerships are permitted, provided that the entity created qualifies as a small business in accordance with the Small Business Act, 15 U.S.C. § 631.

DEFINITION OF A SMALL BUSINESS

A small business concern is one that, at the time of award of Phase I and Phase II, meets all of the criteria established by the Small Business Administration which are published in 13 C.F.R § 121.701-705, repeated here for clarity. A small business concern is one that, at the time of award of Phase I and Phase II, meets all of the following criteria:

a. Is independently owned and operated, is not dominant in the field of operation in which it is proposing, has a place of business in the United States and operates primarily within the United States or makes a significant contribution to the US economy, and is organized for profit.

b. Is (1) at least 51% owned and controlled by one or more individuals who are citizens of, or permanent resident aliens in, the United States, or (2) it must be a for-profit business concern that is at least 51% owned and controlled by another for-profit business concern that is at least 51% owned and controlled by one or more individuals who are citizens of, or permanent resident aliens in, the United States.

c. Has, including its affiliates, an average number of employees for the preceding 12 months not exceeding 500, and meets the other regulatory requirements found in 13 CFR Part 121. Business concerns are generally considered to be affiliates of one another when either directly or indirectly, (1) one concern controls or has the power to control the other; or (2) a third-party/parties controls or has the power to control both.

Control can be exercised through common ownership, common management, and contractual relationships. The term "affiliates" is defined in greater detail in 13 CFR 121.103. The term "number of employees" is defined in 13 CFR 121.106.

A business concern may be in the form of an individual proprietorship, partnership, limited liability company, corporation, joint venture, association, trust, or cooperative. Further information may be obtained at http://sba.gov/size or by contacting the Small Business Administration's Government Contracting Area Office or Office of Size Standards.

DESCRIPTION OF THE OSD SBIR THREE-PHASE PROGRAM

Phase I is to determine, insofar as possible, the scientific or technical merit and feasibility of ideas submitted under the SBIR Program and will typically be one half-person year effort over a period not to exceed six months, with a dollar value up to $150,000. Proposals are evaluated using the Phase I evaluation criteria, in accordance with Section 6.0 of the DoD Program Solicitation. Proposals should concentrate on research and development which will significantly contribute to proving the scientific and technical feasibility of the proposed effort, the successful completion of which is a prerequisite for further DoD support in Phase II. The measure of Phase I success includes technical performance toward the topic objectives and evaluations of the extent to which Phase II results would have the potential to yield a product or process of continuing importance to DoD and the private sector.

Subsequent Phase II awards will be made to firms on the basis of results from the Phase I effort and the scientific and technical merit of the Phase II proposal in addressing the goals and objectives described in the topic. Phase II awards will typically cover two to five person-years of effort over a period generally not to exceed 24 months (subject to negotiation), with a dollar value up to $1,000,000. Phase II is the principal research and development effort and is expected to produce a well-defined deliverable prototype

or process. A more comprehensive proposal will be required for Phase II. In order for a small business to be considered for a Phase II award, the firm must be a recipient of a Phase I award under that topic.

All Phase I awardees will be allowed to submit a Phase II proposal for evaluation and selection. The details on the due date, content, and submission requirements of the Phase II proposal will be provided by the awarding technical point of contact and/or the contracting officer by subsequent notification. All SBIR Phase II awards made on topics from solicitations prior to FY 2013 will be conducted in accordance with the procedures specified in those solicitations (this means by invitation only for those prior topics).

Under Phase III, the DoD may award non-SBIR funded follow-on contracts for products or processes, which meet the Component mission needs. This solicitation is designed, in part, to encourage the conversion of federally sponsored research and development innovation into private sector applications. The small business is expected to use non-federal capital to pursue private sector applications of the research and development.

DoD is not obligated to make any awards under Phase I, II, or III. For specifics regarding the evaluation and award of Phase I or II contracts, please read the DoD Solicitation Instructions very carefully. Phase II proposals will be reviewed for overall merit based upon the criteria in Section 4.3 of this solicitation.

This solicitation is for Phase I proposals only. Any proposal submitted under prior SBIR solicitations will not be considered under this solicitation; however, offerors who were not awarded a contract in response to a particular topic under prior SBIR solicitations are free to update or modify and submit the same or modified proposal if it is responsive to any of the topics listed in this section.

FOLLOW-ON FUNDING

In addition to supporting scientific and engineering research and development, another important goal of the program is conversion of DoD-supported research and development into commercial (both Defense and Private Sector) products. Proposers are encouraged to obtain a contingent commitment for follow-on funding prior to Phase II where it is felt that the research and development has commercialization potential in either a Defense system or the private sector. Proposers who feel that their research and development has the potential to meet Defense system objectives or private sector market needs are encouraged to obtain either non-SBIR DoD follow-on funding or non-federal follow-on funding, for Phase III to pursue commercialization development. The commitment should be obtained during the course of Phase I performance, or early in the Phase II performance. This commitment may be contingent upon the DoD supported development meeting some specific technical objectives in Phase II which if met, would justify funding to pursue further development for commercial (either Defense related or private sector) purposes in Phase III. The recipient will be permitted to obtain commercial rights to any invention made in either Phase I or Phase II, subject to the patent policies stated elsewhere in this solicitation and awarded contract.

OSD SBIR 15.3 Topic Index

OSD153-001	System Architecture Recovery and Analysis (SARA)
OSD153-002	Cyber Deception for Network Defense
OSD153-003	Next-Generation Secured Mobile Devices for Mobile, Tactical Environments
OSD153-004	Moving Target Defense
OSD153-005	High-Assurance Cyber-Physical Systems

OSD SBIR 15.3 Topic Descriptions

OSD153-001 TITLE: System Architecture Recovery and Analysis (SARA)

TECHNOLOGY AREA(S): Information Systems

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), 22 CFR Parts 120-130, which controls the export and import of defense-related material and services, including export of sensitive technical data, or the Export Administration Regulation (EAR), 15 CFR Parts 730-774, which controls dual use items. Offerors must disclose any proposed use of foreign nationals (FNs), their country(ies) of origin, the type of visa or work permit possessed, and the statement of work (SOW) tasks intended for accomplishment by the FN(s) in accordance with section 5.4.c.(8) of the solicitation and within the AF Component-specific instructions. Offerors are advised foreign nationals proposed to perform on this topic may be restricted due to the technical data under US Export Control Laws. Please direct questions to the AF SBIR/STTR Contracting Officer, Ms. Gail Nyikon, gail.nyikon@us.af.mil.

OBJECTIVE: Develop innovative methods, tools and techniques to recover the implemented software architecture of a cyber-physical system in the absence of source code or other program information.

DESCRIPTION: The understanding of the architectural design of a system (such as a nuclear reactor safety system or vehicle operations system) is crucial in assessing the system's security posture and robustness. Even if the original design of a software architecture is known, the implemented architecture may vary due to implementation choices related to performance, efficiency, language constructs, patching, etc. While reverse engineering and binary analysis tools for desktop applications have been developed for some time, tools for embedded applications (e.g., supervisory control and data acquisition (SCADA) systems, industrial control systems (ICS), embedded systems, etc.) are either immature or non-existent. In addition, vulnerability analysis at a software design and source code level cannot uncover all susceptibilities because additional software (e.g., library routines, firmware, etc.) are integrated into the architecture and are potential malware sources.

In order to truly understand weaknesses, a mechanism is needed that can extract the "as-built" architecture from the machine code and achieve a high level of confidence that the recovered architecture representation is accurate. This mechanism should: (1) Identify critical security points in the architecture, (2) discover the functionality of individual system components and (3) enable cyber security engineers to scrutinize critical access points and potential susceptibilities in the system. This technology could be used by systems engineers either to analyze "black box" architectures where the design is unknown, or to verify that a software system has been implemented and performs as designed which, in turn, would make it possible to discover when a system has been compromised and does not function as intended.

A focus on real-time embedded systems and real-time operating systems is highly desirable. A solution that runs on Linux or Windows in a desktop environment and can accept binaries from a variety of operating systems (Linux, Windows, VxWorks, Integrity, LynxOS, etc.) and architectures (ARM, x86, PowerPC, etc.) is more relevant than a solution that is OS and/or architecture specific.

PHASE I: Describe & design creative methods/techniques/tools for recovering and reconstructing architecture of an implemented software system, accurately modeling and displaying the architecture, and assessing its security posture. The result should use common modeling standards (SysML, UML, etc.) where possible.

PHASE II: Develop, implement and validate a prototype tool that utilizes the methods/techniques from Phase I. The prototype(s) should be sufficiently functional to evaluate the effectiveness of the approach on a representative real-world software system. Models produced by the tool should highlight potential cyber access points and weaknesses or susceptibilities in the system. Initial compatibility with a variety of processing architectures is desirable, but the solution may initially focus on one.

PHASE III DUAL USE APPLICATIONS: The ability to accurately model and validate an implemented system architecture for verification and assessment will be an invaluable tool for ensuring the safety and security of DoD systems with additional uses in security and safety sensitive industries such as commercial and civil aviation.

REFERENCES:
1. Li, Lixin, and Chao Wang, “Dynamic Analysis and Debugging of Binary Code for Security Applications,” 2013. Available online at: http://www.ece.vt.edu/chaowang/pubDOC/Li13SymRAS.pdf

2. Cesare, Silvio, “Bugalyze.com – Detecting Bugs Using Decompilation and Data Flow Analysis,” July 27, 2013. Available online at: https://media.blackhat.com/us-13/US-13-Cesare-Bugalyze.com-Detecting-Bugs-Using-Decompilation-WP.pdf

3. Zaddach, Jonas, and Andrei Constin, “Embedded Devices Security and Firmware Reverse Engineering,” July 27, 2013. Available online at: https://media.blackhat.com/us-13/US-13-Zaddach-Workshop-on-Embedded-Devices-Security-and-Firmware-Reverse-Engineering-WP.pdf

4. Dunn, Michael, “Toyota's killer firmware: Bad design and its consequences,” October 28, 2013. Available online at: http://www.edn.com/design/automotive/4423428/2/Toyota-s-killer-firmware--Bad-design-and-its-consequences

KEYWORDS: system, architecture, recovery, analysis, embedded, systems, software, binary, assessment, vulnerability, cyber, security, reverse, engineering, design

TPOC-1: Joshua McCamey
Phone: 937-528-8152
Email: Joshua.McCamey@us.af.mil

OSD153-002 TITLE: Cyber Deception for Network Defense

TECHNOLOGY AREA(S): Information Systems

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), 22 CFR Parts 120-130, which controls the export and import of defense-related material and services, including export of sensitive technical data, or the Export Administration Regulation (EAR), 15 CFR Parts 730-774, which controls dual use items. Offerors must disclose any proposed use of foreign nationals (FNs), their country(ies) of origin, the type of visa or work permit possessed, and the statement of work (SOW) tasks intended for accomplishment by the FN(s) in accordance with section 5.4.c.(8) of the solicitation and within the AF Component-specific instructions. Offerors are advised foreign nationals proposed to perform on this topic may be restricted due to the technical data under US Export Control Laws. Please direct questions to the AF SBIR/STTR Contracting Officer, Ms. Gail Nyikon, gail.nyikon@us.af.mil.

OBJECTIVE: Research and develop technology to provide a cyber deception capability that could be employed by commanders to provide false information, confuse, delay, or otherwise impede cyber attackers to the benefit of friendly forces.

DESCRIPTION: Deception is defined as a "deliberate act perpetrated by a sender to engender in a receiver’s beliefs contrary to what the sender believes is true to put the receiver at a disadvantage.” (1) Military deception is defined as “those actions executed to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.” (2) Military forces have used techniques such as camouflage, feints, chaff, jammers, fake equipment, false messages or traffic, etc. for thousands of years to alter an enemy’s perception of reality.

This effort will examine the typical attack steps of; reconnaissance (where the enemy researches, identifies and selects the target), scanning (where detailed information about the target is obtained allowing a specific attack to be crafted), gaining access (where the attack is carried out), and maintaining access (where the attack evidence is deleted and information is exfiltrated or altered/destroyed) to identify where and how deception technologies can be brought to bear to thwart the objectives of an attack.

It is believed that deception techniques, working in conjunction with normal cyber defense methods, can alter the underlying attack process, making it more difficult, time consuming and cost prohibitive. Some work has already been done in cyber deception technologies; i.e., honeypots are computers designed to attract attackers by impersonating another machine that may be worthy of being attacked, honeynets take that further by simulating a number of computers or a network, and products such as the Deception Toolkit conveys an impression of the defenses of a computer system that are different from what they really are by creating phony vulnerabilities.

Modern day military planners need a capability that goes beyond the current state-of-the-art in cyber deception to provide a system or systems that can be employed by a commander when needed to enable additional deception to be inserted into cyber operations.

PHASE I: 1. Design and develop techniques and technologies that could be employed in a representative scenario based on the criticality of the cyber situation and/or INFOCON status, 2. Conduct a complete comparative analysis and, 3. Conduct a proof-of-feasibility demonstration of key enabling concepts.

PHASE II: 1. Develop and demonstrate a prototype that implements the Phase I methodology, 2. Identify appropriate performance metrics for evaluation, 3. Generate a cost estimate and implementation guidance for both a modest pilot project and fielding at the Air Force, regional Network Operations and Security Center or other suitable command level, and 4. Detail the plan for the Phase III.

PHASE III DUAL USE APPLICATIONS: Cyber deception capability in military or commercial networks.

REFERENCES:
1. Burgoon, J. and Buller, D.," Interpersonal deception: III. Effects of deceit on perceived communication and nonverbal behavior dynamics", Journal of Nonverbal Behavior, vol. 18, no. 2, pp. 155-184, Jun. 1994, http://www.eric.ed.gov/ERICWebPortal/recordDetail?accno=EJ514630?Cached, Retrieved 16 May 2

2. Joint Publication 3-13.4, Military Deception, 31 May 1996

3. McQueen, M. and Boyer, W., "Deception Used for Cyber Defense of Control Systems", INL/CON-08- 15204, Idaho National Laboratory, 2009, http://www.inl.gov/technicalpublications/Documents/4247207.pdf, Retrieved 16 May 2013

4. Tan, K. L. G., Confronting Cyberterrorism with Cyber Deception, Naval Postgraduate School, December 2003, http://www.au.af.mil/au/awc/awcgate/nps/cyber_deception.pdf, Retrieved 16 May 2013

KEYWORDS: Cyber Deception, Military Deception, Digital Deception, Active Cyber Defense

TPOC-1: David Climek
Phone: 315-330-4123
Email: david.climek.1@us.af.mil

OSD153-003 TITLE: Next-Generation Secured Mobile Devices for Mobile, Tactical Environments

TECHNOLOGY AREA(S): Information Systems

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), 22 CFR Parts 120-130, which controls the export and import of defense-related material and services, including export of sensitive technical data, or the Export Administration Regulation (EAR), 15 CFR Parts 730-774, which controls dual use items. Offerors must disclose any proposed use of foreign nationals (FNs), their country(ies) of origin, the type of visa or work permit possessed, and the statement of work (SOW) tasks intended for accomplishment by the FN(s) in accordance with section 5.4.c.(8) of the solicitation and within the AF Component-specific instructions. Offerors are advised foreign nationals proposed to perform on this topic may be restricted due to the technical data under US Export Control Laws. Please direct questions to the AF SBIR/STTR Contracting Officer, Ms. Gail Nyikon, gail.nyikon@us.af.mil.

OBJECTIVE: Develop innovative tools & techniques to secure operation of mobile devices & systems: enable security in real-time systems; establish security in disadvantaged, intermittent, & low-bandwidth environments. Must provide military-grade techniques.

DESCRIPTION: The warfighter needs access to and the ability to dynamically share data in a variety of formats. In addition, they need access to this data no matter where they find themselves in the world; be in the office, a hotel room or in an austere area with suspect communications infrastructure. As such, there exists the need to secure commercial mobile devices for information sharing for multiple levels of classification up to the highest classification levels. These solutions must provide data-at-rest, data-in-transit, tamper mitigation, secure OS and device attestation, dual-factor authentication & authorization, and efficient power consumption.

PHASE I: Describe and develop creative methods, techniques and tools for establishing, guaranteeing and conveying the integrity and authenticity of data via commercial mobile environment. The methodologies should in particular address the issue of how to ensure sensitive data remains isolated according to published NSA guidelines (CSfC and MCP Protection Profiles).

PHASE II: Develop, implement and validate a prototype system that utilizes the tools and methods from Phase I. The prototypes should be sufficiently detailed to evaluate scalability, usability, and resistance to malicious attack. Also should show evidence of efficient power consumption. Efficiency is less critical than overall scalability and security.

PHASE III DUAL USE APPLICATIONS: Provide at least 3 secure containers where applications can execute assurance that will not cross over into other containers resident on the device; show limited performance degradation. This will enable users to utilize commercial mobile apps as well as those specific to government agencies.

REFERENCES:
1. NSA Commercial Solutions for Classified Program: http://www.nsa.gov/ia/programs/csfc_program/

2. NSA Mobile Program/ Mobility Capabilities Package:
http://www.nsa.gov/ia/_files/Mobility_Capability_Pkg_Vers_2_3.pdf

3. National Information Assurance partnership: https://www.niap-ccevs.org/

KEYWORDS: Security, Mobile, Data-at-Rest, Data-In-Transit, dynamic mobile device management

TPOC-1: Michael Mayhew
Phone: 315-330-3913
Email: Michael.Mayhew.1@us.af.mil

OSD153-004 TITLE: Moving Target Defense

TECHNOLOGY AREA(S): Information Systems

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), 22 CFR Parts 120-130, which controls the export and import of defense-related material and services, including export of sensitive technical data, or the Export Administration Regulation (EAR), 15 CFR Parts 730-774, which controls dual use items. Offerors must disclose any proposed use of foreign nationals (FNs), their country(ies) of origin, the type of visa or work permit possessed, and the statement of work (SOW) tasks intended for accomplishment by the FN(s) in accordance with section 5.4.c.(8) of the solicitation and within the AF Component-specific instructions. Offerors are advised foreign nationals proposed to perform on this topic may be restricted due to the technical data under US Export Control Laws. Please direct questions to the AF SBIR/STTR Contracting Officer, Ms. Gail Nyikon, gail.nyikon@us.af.mil.

OBJECTIVE: Develop innovative techniques to adapt network or perception of network to thwart adversary attempt to perform reconnaissance, launch attack and successfully exfiltrate information.

DESCRIPTION: Attackers go through the process of gathering information about a target, preparing the correct and appropriate attack vector, gaining access, maintaining access and then causing harm, including removing information. If we can disrupt the attacker's processes at any of these stages by introducing MTD techniques, we may defeat or at least delay the attack by increasing the attackers work factor and making them become more "visible" and subject to detection and eradication via other techniques. The methods developed should be compatible with existing protocols and standards so that they can be applied to most networks.

The increasing focus on network centric warfare means that the ability to protect networks will become essential to ensuring the safety of military operations. Similarly, in the civilian domain the increased use of electronic commerce and cyber-physical systems, such as industrial/home control networks, is creating a situation where the ability to resist or delay attacks will become more and more critical over time.

PHASE I: Describe & develop creative methods, techniques & tools for causing the perceived/actual picture of the network from an attackers perspective to change. Methodologies should in particular address issues of how to cause disruption & doubt from an attacker's perspective but not add any significant error, confusion/processing to the protected network.

PHASE II: Develop, implement and validate a prototype system that utilizes the tools and methods from Phase I. The prototypes should be sufficiently detailed to evaluate scalability, usability, and resistance to malicious attack. Efficiency is also an issue that should be explored, although it is less critical than overall scalability.

PHASE III DUAL USE APPLICATIONS: Demonstrate results in relevant military and civilian applications.

REFERENCES:
1. Jajodia, S., Ghosh, A.K., Swarup, V., Wang, C., Wang, X.S. (Eds.), "Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats", Springer, NY, 2011, ISBN 978-1-4614-0977-9

2. Jafarian, J., Al-Shaer, E., Duan, Q., "OpenFlow Random Host Mutation: Transparent Moving Target Defense using Software Defined Networking", Retrieved from http://www.ece.cmu.edu/~ece739/papers/movingtarget.pdf

3. Vikram, S., Yang, C., Gu, G., "NOMAD: Towards Non-Intrusive Moving-Target Defense against Web Bots", Retrieved from http://faculty.cse.tamu.edu/guofei/paper/NOMAD_CNS13.pdf

KEYWORDS: moving target defense, agility, uncertainty, dynamic diversity defense

TPOC-1: David Climek
Phone: 315-330-4123
Email: david.climek.1@us.af.mil

OSD153-005 TITLE: High-Assurance Cyber-Physical Systems

TECHNOLOGY AREA(S): Information Systems

OBJECTIVE: To define threat models; develop and prototype novel, resilient architectures, tools, and techniques to mitigate threats to cyber-physical system. To develop modeling and simulation tools that consider the safety and correctness constraints of the physical systems and the interaction with the digital components.

DESCRIPTION: Cyber-physical systems integrate computational, networking, and physical resources. Popular examples include industrial control systems, medical safety systems, software defined radios, and avionics systems. The computational and networking resources provide many benefits to the control of physical systems. The computational resources allow for re-programmability, meaning that bugs in the design can be addressed on deployed systems, without the need for costly hardware replacements. Networking these devices further increases the ease of re-programmability, since the operators are no longer required to physically visit every node that needs re-programmed. However, with the increased benefits come many additional challenges and increased threats.

While the benefits of re-programmability and networked nodes are hard to argue, the increased attack surface from these additional benefits must be carefully considered, especially for safety-critical systems. The ability for an adversary to remotely connect to, and re-program, a control device for a safety system poses a significant risk. What is needed are tools, techniques, and systems that are resilient to these remote adversaries, as well as other types of failures.

PHASE I: Perform a study to describe the tools, techniques, and/or architectures in need of development for cyber-physical systems in order to limit an adversary's, or component failure's, impact, and allow the cyber-physical system to continue to operate in a degraded mode, while still maintaining the safety properties of the system. The study should include plans for a Phase II prototype hardware or software module that demonstrates the enhanced resilience of the CPS.

PHASE II: Develop, implement, and validate a prototype system that utilizes the architecture, tools, and methods from Phase I. The prototypes should be sufficiently detailed to evaluate scalability, usability, and resilience to attack, or failure. Efficiency of the architecture is important, especially, in safety critical applications. Develop novel techniques and tools for modelling CPS, allowing for modeling/simulation of the system to ensure safety and correctness of the controls.

PHASE III DUAL USE APPLICATIONS: Safety-critical control systems span a wide range of industrial and military applications. Any enhancements to the security of commercial-off-the-shelf (COTS) control systems hardware and software will have benefits to both military and commercial markets. Transition of this technology would benefit DoD programs such as SPYDER, MNVR and Rifleman Radios, as well as the TACDIS Cross Domain Solution and the Hardware Convergence R&D initiative.

REFERENCES:
1. Overview of Cyber Physical Systems available online at http://cyberphysicalsystems.org/

2. Report of the President's Council of Advisors on Science and Technology (PCAST) titled Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology available at http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd-report-2010.

3. A Trusted Safety Verifier for Process Controller Code. Stephen McLaughlin, Devin Pohly, Patrick McDaniel, and Saman Zonouz. Proceedings of ISOC Network and Distributed Systems Security Symposium (NDSS 2014).

4. CPS: Stateful Policy Enforcement for Control System Device Usage, Stephen McLaughlin. Proc. 29th Annual Computer Security Applications Conference (ACSAC 2013) CPS Track

KEYWORDS: cyber-physical systems, high-assurance architectures, safety systems, industrial control systems, embedded systems, resilience

TPOC-1: Humza Shahid
Phone: 443-395-5703
Email: Humza.shahid.civ@mail.mil

TPOC-2: Jonathon Santos
Phone: 443-395-5706
Email: Jonathan.M.Santos.civ@mail.mil